Patch Release Note

Patch 86253-04
For Rapier Series Switches

Introduction

This patch release note lists the issues addressed and enhancements made in patch 86253-04 for Software Release 2.5.3 on existing models of Rapier series switches. Patch file details are listed in Table 1.

Table 1: Patch file details for Patch 86253-04.

Base Software Release File	86s-253.rez
Patch Release Date	17-October-2003
Compressed Patch File Name	86253-03.paz
Compressed Patch File Size	585295 bytes

This release note should be read in conjunction with the following documents:

- Release Note: Software Release 2.5.3 for Rapier Switches and AR400 and AR700 Series Routers (Document Number C613-10362-00 Rev A) available from *www.alliedtelesyn.co.nz/documentation/documentation.html*.
- Rapier Switch Documentation Set for Software Release 2.5.1 available on the Documentation and Tools CD-ROM packaged with your switch, or from *www.alliedtelesyn.co.nz/documentation/documentation.html*.

WARNING: Using a patch for a different model or software release may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesyn International. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesyn International can not accept any type of liability for errors in, or omissions arising from the use of this information.

Some of the issues addressed in this Release Note include a level number. This number reflects the importance of the issue that has been resolved. The levels are:

Level 1 This issue will cause significant interruption to network services, and there is no work-around.

Level 2 This issue will cause interruption to network service, however there is a work-around.

Level 3 This issue will seldom appear, and will cause minor inconvenience.

Level 4 This issue represents a cosmetic change and does not affect network operation.

Features in 86253-04

Patch 86253-04 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.3, and the following enhancements:

PCR: 02414 Module: IPV6, SWI, IPG, VLAN

MLD snooping is now supported on AT-9800 Series Switches and Rapier *i* Series Switches. For details, see "*MLD Snooping*" on page 17.

PCR: 02577 Module: IPG, LOG Level: 4

The ability to log MAC addresses whenever the ARP cache changes has been added. To enable this, use the command:

```
ENABLE IP ARP LOG
```

To disable it, use the command:

```
DISABLE IP ARP LOG
```

The logging of MAC addresses is disabled by default. Use the SHOW LOG command to view the MAC addresses that have been logged when the ARP cache changes.

PCR: 03162 Module: IPV6 Level: 3

The performance of IPv6 has been improved by introducing IPv6 flows.

PCR: 03268 Module: SWI Level: 1

When using MVR on a Rapier 48 or Rapier 48*i*, multicast packets were not forwarded correctly between ports 1-24 and 25-48. This issue has been resolved.

PCR: 03409 Module: SWI Level: 2

The switch filter was not operating correctly after a boot cycle. This issue has been resolved.

PCR: 03524 Module: OSPF, IPG Level: 2

OSPF disabled RIP unless RIP was activated using the SET OSPF RIP command. This issue has been resolved.

PCR: 03560 Module: IPV6 Level: 2

A fatal error sometimes occurred when IPv6 multicast packets were forwarded via an interface that went down and then came back up. This issue has been resolved.

PCR: 03598 Module: ETH, IPG, IPv6, IPX, PORT, PPP. Level: 3

After about 250 days, commands such as SHOW BRIDGE COUNT were not displaying the correct number of seconds for *Uptime* and *Last Change At*. days. This issue has been resolved.

PCR: 03616 Module: IPG Level: 4

Three new commands have been added to enable and disable transmission of the following ICMP messages: *Network Unreachable*, *Host Unreachable,* and all *Redirect* messages.

The commands are:

```
DISABLE IP
   ICMPREPLY[={ALL|NETUNREACH|HOSTUNREACH|REDIRECT}]

ENABLE IP
   ICMPREPLY[={ALL|NETUNREACH|HOSTUNREACH|REDIRECT}]

SHOW IP ICMPREPLY
```

For details, see "*Enable and Disable ICMP Messages*" on page 14.

PCR: 03622 Module: ENCO Level: 2

Interoperating with other vendors implementations of ISAKMP was occasionally causing errors following key exchanges. This relates to differing implementations of the RFC regarding the retention of leading zeros. This issue has been resolved by modifying the software to retain leading zeros. An additional command provides compatibility with routers that still use previous software versions. The command details are:

```
SET ENCO DHPADDING={ON|OFF}
```

This command controls the padding process for Diffie Hellman generated values. This may be required when interoperability is required with other vendor's equipment that uses the Diffie Hellman algorithm.

The DHPADDING parameter specifies whether the Diffie Hellman generated values should be padded or not. If ON is specified, then leading zeros will be inserted into the generated values. If OFF is specified, then the generated values will not be padded. The default is ON.

For example, to turn off the Diffie Hellman padding, use the command:

```
SET ENCO DHPADDING=OFF
```

Also, the output of the SHOW ENCO command now contains a new line showing the setting for DHPADDING.

PCR: 03704 Module: BGP Level: 2

BGP was importing the best route from IP without checking whether the route was *reachable*. BGP now selects the best *reachable* route. If there are no *reachable* routes, BGP will select the best *unreachable* route.

PCR: 03710 Module: PIM, PIM6 Level: 2

The list of multicast groups for each Rendezvous Point occasionally became corrupted, and this could cause a fatal error. This issue has been resolved.

PCR: 03723 Module: BGP Level: 2

BGP routes that were added after a summary aggregate route had been formed were not suppressed. This issue has been resolved: all routes added after summary aggregate route creation are also now suppressed.

The SHOW BGP ROUTE command displayed unselected routes as the "best" route, until they had been processed. This issue has been resolved.

When a single route was deleted from an aggregate route, the aggregate route was deleted, even if it contained other routes. This issue has been resolved.

PCR: 03726 Module: TTY, USER Level: 3

The time recorded when a user logged in was overwritten when the same user logged in a second time while the original connection was still active. This meant the SHOW USER command displayed the same time for both connections. This issue has been resolved.

PCR: 03733 Module: IPV6 Level: 3

When an oversize packet (PMTU) was received, an error message was not returned, even when IPv6 flow was enabled. This issue has been resolved.

PCR: 03734 Module: IPG Level: 2

With static multicasting enabled on two VLANs, only the first few multicast packets of a stream were L3 forwarded. This issue has been resolved.

PCR: 03751 Module: MLDS Level: 3

The MLD snooping entries registered on a port were not removed when the port went down or was unplugged. This issue has been resolved.

PCR: 03757 Module: BGP Level: 2

Route flapping occurred with BGP when an interface went down. This issue has been resolved.

PCR: 03771 Module: SWI Level: 2

When ingress rate limiting was used on Rapier switch ports, TCP sessions sometimes obtained a throughput that was lower than the configured ingress rate limit. This issue has been resolved.

PCR: 03780 Module: INSTALL Level: 3

If a configuration file had a long file name, the SHOW CONFIG command displayed the file name using the shortened DOS 8.3 format (where file names are 8 characters long, with extensions of 3 characters). This issue has been resolved so that long configuration file names are now displayed using the DOS 16.3 format (where file names are up to 16 characters long).

PCR: 03789 Module: ETH Level: 2

When a 4-port ETH PIC card was installed, the output of the SHOW IP INTERFACE command showed the ETH port as Down, but the link LEDs on the card were lit. This issue has been resolved. The SHOW command now shows the correct link status. The link will go down after 90 seconds if no inbound traffic is received. When inbound traffic is received the link will come up.

PCR: 03790 Module: SWI Level: 2

When a tagged port was deleted from a VLAN that was in the default STP, and the port was then added to the VLAN again, communications were sometimes not resumed on that port. This issue has been resolved.

PCR: 03798 Module: IKMP Level: 3

ISAKMP did not support the IPSec message option *ID_IPV6_ADDR_SUBNET* (RFC 2407, 4.6.2.7). ISAKMP was using the *ID_IPV6_ADDR* (RFC 2407, 4.6.2.6) option instead. This issue has been resolved.

PCR: 03801 Module: MLDS Level: 2

MLD and MLD Snooping accepted MLD *Query* packets with a hop limit greater than 1. Duplicate packets were forwarded when the hop limit was not 1 and the payload was 0::0. This issue has been resolved. MLD and MLD Snooping now require the hop limit to be 1.

PCR: 03806 Module: VRRP Level: 4

After the SHOW VRRP command was executed, incorrect trigger messages were entered into the log. This issue has been resolved.

PCR: 03809 Module: SWI Level: 2

An additional check has been added for unknown GBIC models to determine if they are copper or fibre.

PCR: 03817 Module: IPV6 Level: 2

A fatal error occurred when IPv6 fragmented a packet. Also, when a large fragmented ICMP echo request packet was received, the reply may not have been fragmented and so may have exceeded the MTU for the interface it was sent on. These issues have been resolved.

PCR: 03826 Module: BGP Level: 2

When BGP imported routes from IP with the ADD BGP IMPORT command, and there were multiple import choices, the best IP route was not always imported. This issue has been resolved.

PCR: 03828 Module: IPV6 Level: 2

The MTU value for IPv6 PPP interfaces was always set to 1280 bytes. This MTU value is now correctly set to 1500 bytes, and 1492 bytes for PPP over Ethernet (PPPoE).

PCR: 03836 Module: OSPF Level: 2

OSPF sometimes chose routes with an infinite metric over routes with a finite metric when selecting the best local route. This issue has been resolved.

PCR: 03839 Module: IPV6 Level: 2

A fatal error sometimes occurred when an IPv6 ping packet length exceeded 1453 bytes. This issue has been resolved.

PCR: 03843 Module: DHCP Level: 2

When some DHCP entries were in *Reclaim* mode, and all interface links related to the range of these entries went down, these DHCP entries were stuck in *Reclaim* mode. This issue has been resolved.

PCR: 03847 Module: TTY Level: 3

Entering Ctrl-N caused some terminals to expect Shift Out ASCII characters. This issue has been resolved.

PCR: 03850 Module: FFS Level: 3

Files were not displayed in the SHOW FFILE command output, after entering "Q" at the CLI to quit from a previous prompt. This issue has been resolved.

PCR: 03852 Module: IPG, IPV6 Level: 2

PIM SM did not establish a BSR candidate between two AR720 routers with PPP over SYN. This issue has been resolved.

PCR: 03854 Module: SWI Level: 2

When INGRESSLIMIT parameter in the SET SWITCH PORT command was set to 64kbps, the switch received packets intermittently rather than continuously. This issue has been resolved.

PCR: 03855 Module: IPG Level: 2

Previously, an IP multicast stream destined for an IP multicast group was forwarded out ports in the All Groups IGMP snooping entry even after this entry had timed out. This issue has been resolved.

PCR: 03861 Module: IPV6 Level: 2

When a connector was plugged into one physical interface, the RIPng request packet was erroneously transmitted from all interfaces on the switch. This issue has been resolved.

PCR: 03864 Module: BGP Level: 2

BGP sent *Update* packets when the local host route table changed but did not affect BGP. Also, BGP did not send *Withdrawn* packets when there was a change in the best route. These issues have been resolved.

PCR: 03867 Module: BGP Level: 2

BGP sometimes chose routes with an infinite metric over routes with a finite metric when selecting the best local route. This issue has been resolved.

PCR: 03868 Module: IPG Level: 3

The *ipForwDatagrams* SNMP MIB object was incremented when it should not have been. This issue has been resolved.

PCR: 03870 Module: SWI, VLAN Level: 3

On Rapier 48*i* switches, mirror port information was repeated in the output of the SHOW VLAN command. This issue has been resolved.

PCR: 03871 Module: FIREWALL Level: 2

The HTTP proxy sometimes allowed URL requests that should have been denied. Also, the HTTP proxy denied all URLs that contained a deniable keyword, even when some URLs with that word had explicitly been allowed. These issues have been resolved.

PCR: 03874 Module: DHCP Level: 3

For parameters that accept a list of IP addresses in a DHCP command (such as LOGSERVER in the ADD DHCP POLICY command), the list is now limited to a maximum of 32 IP addresses.

PCR: 03875 Module: IPG Level: 2

Sometimes OSPF routes were not entered in the IP route table. This issue has been resolved.

PCR: 03876 Module: PING Level: 2

A fatal error occurred if the TRACE command was executed when a trace was already in progress. This issue has been resolved.

PCR: 03878 Module: SWI Level: 2

The layer 3 filter was matching a layer 3 packet incorrectly when the egress port was specified by the filter. This issue has been resolved.

PCR: 03883 Module: IPG Level: 3

Some IP addresses were not displayed correctly in log messages. This issue has been resolved.

PCR: 03884 Module: IPG Level: 2

The IGMP MVR membership timeout was not operating correctly. Membership of a multicast group is now eliminated when it times out. Also, *Leave* messages were not being processed correctly, which sometimes delayed the membership timeout. These issues have been resolved.

PCR: 03888 Module: DHCP, TELNET Level: 2

When the device was configured as a DHCP server, a fatal error sometimes occurred when a telnet session to the device was closed while DHCP was reclaiming IP addresses. Also, a telnet error message displayed an incorrect value when a telnet command line parameter was repeated (for example, SHOW TELNET TELNET). These issues have been resolved.

PCR: 03890 Module: IGMP, SWI Level: 2

The switch was adding a router port for multicast packets to destinations with an address in the range 224.0.0.x. Switch port entries are now only created for special router multicast addresses.

PCR: 03895 Module: DHCP Level: 2

If the DHCP server had a policy name greater than 5 characters long, and a very long MERITDUMP or ROOTPATH value, the device could not correctly create the configuration. This issue has been resolved.

PCR: 03896 Module: TTY Level: 3

A fatal error occurred when a long string of text was pasted over an existing long string of text at the CLI. This issue has been resolved.

PCR: 03898 Module: ETH Level: 3

An ETH interface was sometimes shown as *Up* in the output of the SHOW INTERFACE command when it was actually *Down*. This issue has been resolved.

PCR: 03902 Module: FIREWALL Level: 3

Under some circumstances traffic did not have NAT applied if a standard subnet NAT rule was added to a public interface. Such rules did not correctly match incoming traffic when the REMOTEIP parameter in the ADD FIREWALL POLICY RULE command was not specified, and the destination IP address was not the interface's actual IP address. If this situation occurred, traffic was redirected back out the public interface. This issue has been resolved.

PCR: 03906 Module: SWITCH Level: 2

Software emulation of layer 3 hardware filtering was not operating correctly. Packets that the switch had no routing information for were filtered incorrectly. The first packet of a flow that should have been dropped was not dropped, and a flow that should have been allowed was being dropped. This issue has been resolved.

PCR: 03907 Module: IPV6 Level: 2

The CREATE CONFIG command did not generate the TYPE parameter for ADD IPV6 INTERFACE commands. This issue has been resolved.

PCR: 03911 Module: SWI Level: 3

The ADD SWITCH FILTER command returned an incorrect error message if a broadcast address was specified for the DESTINATION parameter. This issue has been resolved.

PCR: 03914 Module: IPG, VLAN Level: 3

When IGMP snooping was disabled with the DISABLE IGMPSNOOPING command, IGMP packets were not flooded. This issue has been resolved.

PCR: 03921 Module: IP ARP Level: 3

ARP requests with invalid source MAC and IP addresses were being processed, but should have been dropped. This issue has been resolved.

PCR: 03925 Module: IPV6 Level: 3

Incorrect debug information was returned when an ICMPv6 *PacketTooBig* message was received. This issue has been resolved.

PCR: 03928 Module: IKMP Level: 2

ISAKMP in *aggressive* mode did not establish a connection when the peer client sent 10 or more payloads. This issue has been resolved.

PCR: 03931 Module: IPSEC Level: 3

The IPSec configuration was not created correctly when the RADDRESS and LNAME parameters in the CREATE IPSEC POLICY command were used together. This issue has been resolved.

PCR: 03934 Module: IPSEC Level: 2

The CREATE IPSEC POLICY command failed if the interface specified with the INTERFACE parameter did not have a global IPv6 interface defined. This PCR implements a workaround by using the interface's link-local IPv6 address if no other IPv6 address can be found.

PCR: 03935 Module: ISAKMP Level: 3

ISAKMP debug messages now correctly output IPv6 addresses when using IPv6, and IPv4 addresses when using IPv4.

PCR: 03936 Module: IKMP Level: 3

When ISAKMP was used with IPv6, an incorrect IP address was displayed in the output of the SHOW ISAKMP EXCHANGE command. This issue has been resolved.

PCR: 03938 Module: IKMP Level: 3

DHEXPONENTLENGTH parameter in the CREATE ISAKMP POLICY command was not accepted when creating ISAKMP policies that used IPv6. This issue has been resolved.

PCR: 03939 Module: IPV6 Level: 2

When a *NeighbourAdvert* message containing an anycast target address was received, the device incorrectly performed Duplicate Address Detection. This issue has been resolved.

PCR: 03946 Module: IPSEC Level: 3

When IPSec was used with IPv6, an incorrect IP address was displayed in the output of the SHOW IPSEC SA command. This issue has been resolved.

PCR: 03949 Module: IPSEC Level: 3

If a local IP address and remote IP address were not specified in the CREATE IPSEC POLICY command for IPv6 IPSec, the SET IPSEC POLICY configuration was shown unnecessarily in the output of the SHOW CONFIG DYNAMIC=IPSEC command. This issue has been resolved.

PCR: 03952 Module: SWI Level: 3

MAC address are now deleted from the all the internal tables for ports where the learn limit has been exceeded.

PCR: 03954 Module: IPV6 Level: 2

An anycast address could not be assigned when the prefix for the anycast address had previously been assigned on that interface. This issue has been resolved.

PCR: 03958 Module: FIREWALL Level: 2

The ADD FIREWALL POLICY RULE and SET FIREWALL POLICY RULE commands no longer accept the GBLREMOTEIP parameter with standard NAT, or enhanced NAT for a private interface.

PCR: 03965 Module: IPSEC Level: 3

IPv6 used the same SA soft expiry timer at both ends of a link, which used memory unnecessarily. This issue has been resolved.

PCR: 03971 Module: SWI Level: 1

A change made in patch 86253-03 caused the Rapier 48 to unexpectedly reboot continuously when powered up. This issue has been resolved.

PCR: 03973 Module: IPG Level: 3

When equal cost multipath routes were used, the IP option field for trace route was not applied correctly. This issue has been resolved.

PCR: 03986 Module: BGP, IPG Level: 2

Route flapping occurred if an interface went down and there was another route to that interface's next hop. This issue has been resolved.

PCR: 31001 Module: DHCP Level: 2

When executing the SET DHCP POLICY, DELETE DHCP POLICY and DESTROY DHCP POLICY commands, memory was not de-allocated correctly. This issue has been resolved.

PCR: 31013 Module: SWI Level: 2

If ports were set to a speed of 100m when creating a switch trunk, the speed could not subsequently be set to 1000m, even if the ports were capable of that speed. This issue has been resolved.

PCR: 31015 Module: STP Level: 2

The PORT and PORTPRIORITY parameters of the STP PORT command were not always updating switch instances on ports that are members of multiple STP instances. This issue has been resolved.

PCR: 31017 Module: NTP Level: 3

The *RootDispersion* value in NTP packets was negative. RFC 1305 states that only positive values greater than zero are valid. This issue has been resolved.

PCR: 31019 Module: PIM6 Level: 2

The checksum for the PIMv2 *Register* message for IPv6 was not being calculated correctly. This issue has been resolved.

PCR: 031020 Module: PIM Level: 2

When the switch received a generation ID change message, it was not responding by sending a PIM HELLO message. This issue has been resolved.

PCR: 31028 Module: BGP Level: 2

BGP did not always send *Withdrawn* advertisements when a route went down. This issue has been resolved.

PCR: 31069 Module: IPV6 Level: 2

When adding an IPv6 filter, an error message was displayed stating that the source IP address was not specified, even when the address was specified. This issue has been resolved.

Features in 86253-03

Patch file details are listed in Table 2:

Table 2: Patch file details for Patch 86253-03.

Base Software Release File	86s-253.rez
Patch Release Date	30-July-2003
Compressed Patch File Name	86253-03.paz
Compressed Patch File Size	191102 bytes

Patch 86253-03 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.3, and the following enhancements:

PCR: 03816 Module: IPG Level: 2

When ports were added or removed as a range with the ENABLE IP IGMP ALLGROUPS and DISABLE IP IGMP ALLGROUPS commands, port values were interpreted as 2 separate ports. This issue has been resolved.

Features in 86253-02

Patch file details are listed in Table 3:

Table 3: Patch file details for Patch 86253-02.

Base Software Release File	86s-253.rez
Patch Release Date	25-July-2003
Compressed Patch File Name	86253-02.paz
Compressed Patch File Size	190900 bytes

Patch 86253-02 includes the following enhancements and resolved issues:

PCR: 03420 Module: IPG, SWI Level: 3

It is now possible to prevent specified ports from acting as IGMP all-group ports, and specify which ports are allowed to behave as all-group entry ports. This is enabled with the ENABLE IP IGMP ALLGROUP command, and disabled with the DISABLE IP IGMP ALLGROUP command.

For details, see "*IGMP Snooping All-Group Entry*" on page 17.

PCR: 03515 Module: DHCP Level: 3

DHCP was offering network and broadcast addresses to clients. This issue has been resolved.

PCR: 03609 Module: OSPF Level: 1

The IP route filter did not always work correctly for OSPF. This issue has been resolved.

PCR: 03657 Module: SWI Level: 3

Executing the DISABLE SWITCH PORT command on a port that was the source of a mirror port did not disable the mirror port. This issue has been resolved.

PCR: 03691 Module: DVMRP Level: 2

A fatal error occurred if the number of DVMRP interfaces being added exceeded the limit. This issue has been resolved.

PCR: 03692 Module: BGP Level: 2

Occasionally a fatal exception may have occurred when sending BGP aggregate routes. This issue has been resolved.

PCR: 03696 Module: IPG Level: 2

IGMP snooping entries were not being deleted from the hardware table. This issue has been resolved. Also, port timers are now updated when the IGMP timeout is changed.

PCR: 03698 Module: DVMRP Level: 3

The output of the SHOW DVMRP FORWARDING command did not display the forwarding ports. This issue has been resolved.

PCR: 03707 Module: STP Level: 2

When adding a port to a VLAN, any STP ports that had been disabled in the default STP were re-enabled. This issue has been resolved.

PCR: 03708 Module: DHCP Level: 2

When the DELETE DHCP RANGE command was executed, DHCP attempted to reclaim the addresses in that range. It also tried to reclaim addresses in that range that were not allocated at that time, resulting in duplicate addresses appearing on the free list for allocation. This has been resolved by allowing DHCP to reclaim only those addresses that are currently in use by one of its clients.

PCR: 03720 Module: STP Level: 2

When changing from RSTP to STP mode, the STPCOMPATIBLE option for the RSTPTYPE parameter incorrectly appeared in the dynamic configuration. Also, when changing from RSTP to STP mode or vice versa, disabled STP ports did not remain in the disabled state. These issues have been resolved.

PCR: 03738 Module: IPG Level: 2

If a port went down, the port was deleted from the appropriate static IGMP associations but was not added back again when it came back up. Similarly, static IGMP associations were automatically deleted but not added back when IP or IGMP was disabled. These issues have been resolved. You can now create IGMP associations before enabling IGMP, and they will become active when IGMP is enabled.

PCR: 03741 Module: FIREWALL Level: 3

The maximum number of firewall sessions had decreased since software release 86s-241. This issue has been resolved.

PCR: 03742 Module: IPV6 Level: 2

Previously, an incorrect source address was used for router advertisements that were sent over an IPv6 tunnel. The source address of the tunnel (specified by the IPADDRESS parameter of the ADD IPV6 TUNNEL command) was used instead of a link local address. This caused an interoperability problem, which has been resolved. Now, if the specified IP address is not a link local address, then a link local address will be created based on the IPv4 tunnel source address and used for router advertisements.

PCR: 03743 Module: IP Level: 3

If a ping was active and the IP configuration was reset, subsequent pings were sent out the wrong interface. This issue has been resolved.

PCR: 03744 Module: PING Level: 3

Executing a ping to the IP address 0.0.0.0 did not return an `invalid destination address` error message. Also, when the TRACE command was executed for local addresses, it timed out after 90 seconds. These issues have been resolved.

PCR: 03764 Module: IPG Level: 3

The IP multicast counter did not increment when IGMP, DVMRP and PIM packets were transmitted and received. This issue has been resolved.

PCR: 03766 Module: FIREWALL Level: 2

The firewall denied streaming data using Windows Media Player 9. This issue has been resolved.

PCR: 03779 Module: DHCP Level: 2

The DHCP client was not honouring a subnet option provided by the DHCP server. This issue has been resolved.

PCR: 03783 Module: IPG Level: 3

The TIMEOUT and SIZE parameters are only valid for the SET IP DNS CACHE command, but no error message was returned if either parameter was specified for the SET IP DNS command. This issue has been resolved.

PCR: 03784 Module: IPV6 Level: 3

Fragmentation of IPv6 packets now complies with RFC 2460's requirement to align packet sizes to 8 octets.

PCR: 03788 Module: DHCP Level: 2

The DHCP server did not send a *DHCPNAK* message when a previously statically assigned IP DHCP entry was again requested by a client. This issue has been resolved.

PCR: 03793 Module: RSVP Level: 3

The ENABLE RSVP INTERFACE command did not succeed if IP was enabled after the RSVP interface had been created. Now, ENABLE RSVP INTERFACE will succeed regardless of when IP is enabled as long as an IP interface exists.

PCR: 03799 Module: DHCP Level: 3

When a new static entry was allocated to a client, an old dynamic entry remained *inuse* for a full lease period. This issue has been resolved. The old entry will now be reclaimed when the client attempts to renew its lease and receives the new static entry.

Enable and Disable ICMP Messages

The *Internet Control Message Protocol* (ICMP) allows routers to send error and control messages to other routers or hosts. It provides the communication between IP software on one system and IP software on another.

This enhancement allows the switch to enable or disable some ICMP messages when directed by the network manager.

The ICMP messages that are able to be enabled or disabled are:

- Network unreachable (RFC792 Type 3 Code 0)
- Host unreachable (RFC792 Type 3 Code 1)
- ICMP redirect messages (RFC792 Type 5 Code 0, 1, 2, 3)

Network Unreachable

This message indicates that the switch does not know how to reach the destination network.

Host Unreachable

This message indicates that the switch does not know how to reach the host.

ICMP Redirect

This message is sent to a local host to tell it that its target is located on the same LAN (no routing is required) or when it detects a host using a non-optimal route (usually because a link has failed or changed its status) on a directly connected router to advise of a better route to a particular destination.

For more information on ICMP, see the IP Chapter in your switch's Software Reference manual.

Commands

This enhancement introduces three new commands:

- DISABLE IP ICMPREPLY
- ENABLE IP ICMPREPLY
- SHOW IP ICMPREPLY

DISABLE IP ICMPREPLY

Syntax

```
DISABLE IP
   ICMPREPLY[={ALL|NETUNREACH|HOSTUNREACH|REDIRECT}]
```

Description This command disables ICMP reply messages.

If ALL is specified, all configurable ICMP message replies are disabled. If NETUNREACH is specified, all network unreachable message replies are disabled (RFC792 Type 3 Code 0). If HOSTUNREACH is specified, all host unreachable message replies are disabled (RFC792 Type 3 Code 1). If REDIRECT is specified, all ICMP redirect message replies are disabled (RFC792 Type 5 Code 0, 1, 2, 3).

Example To disable all configurable ICMP messages, use the command:

```
DISABLE IP ICMPREPLY=ALL
```

See Also ENABLE IP ICMPREPLY
DISABLE IP ECHOREPLY
SHOW IP ICMPREPLY

ENABLE IP ICMPREPLY

Syntax

```
ENABLE IP
   ICMPREPLY[={ALL|NETUNREACH|HOSTUNREACH|REDIRECT}]
```

Description This command enables ICMP reply messages.

If ALL is specified, all configurable ICMP message replies are enabled. If NETUNREACH is specified, all network unreachable message replies are enabled (RFC792 Type 3 Code 0). If HOSTUNREACH is specified, all host unreachable message replies are enabled (RFC792 Type 3 Code 1). If REDIRECT is specified, all ICMP redirect message replies are enabled (RFC792 Type 5 Code 0, 1, 2, 3).

Example To enable all configurable ICMP messages, use the command:

```
ENABLE IP ICMPREPLY=ALL
```

See Also ENABLE IP ECHOREPLY
DISABLE IP ICMPREPLY
SHOW IP ICMPREPLY

SHOW IP ICMPREPLY

Syntax

```
SHOW IP ICMPREPLY
```

Description This command display the status of configurable ICMP messages (Figure

Figure 1: Example output from the SHOW IP ICMPREPLY command:

```
SHOW IP ICMP REPLY MESSAGES
-------------------------------------------------------------------------------
ICMP REPLY MESSAGES:
  Network Unreachable ............... disabled
  Host Unreachable .................. disabled
  Redirect .......................... enabled
-------------------------------------------------------------------------------
```

Table 4: Parameters in the output of the SHOW IP ICMPREPLY command.

Parameter	Meaning
ICMP Reply Messages	A list of ICMP configurable reply messages and whether they are enabled or disabled.

MLD Snooping

Multicast Listener Discovery (MLD) snooping enables the switch to forward IPv6 multicast traffic intelligently, instead of flooding it out all ports in the VLAN. With MLD snooping, the switch passively listens to MLD joins/reports and leaves/done messages, to identify the switch ports that have received joins and/or leaves from devices attached to them. Multicast traffic will only be forwarded to those ports. MLD snooping will also identify ports that are connected to another router or switch and forward messages out those ports appropriately.

MLD snooping is performed at Layer 2 on VLAN interfaces automatically. By default, the switch will only forward traffic out those ports with routers or IPv6 multicast listeners, therefore it will not act as a simple hub and flood all IPv6 multicast traffic out all ports. MLD snooping is independent of the MLD and Layer 3 configuration, so an IPv6 interface does not have to be attached to the VLAN, and MLD does not have to be enabled or configured.

MLD snooping is enabled by default. To disable it, use the command:

```
DISABLE MLDSNOOPING
```

Note that IPv6 multicast packets will flood the VLAN when MLD snooping is disabled.

To enable MLD snooping, use the command:

```
ENABLE MLDSNOOPING
```

To display debugging information, use the command:

```
ENABLE MLDSNOOPING DEBUG
```

This command displays the ports that are currently receiving MLD packets and the ports that are being added or taken off the switch's multicast group membership registration.

To disable debugging, use the command:

```
DISABLE MLDSNOOPING DEBUG
```

To display information about MLD snooping, use the command:

```
SHOW MLDSNOOPING COUNTER
```

For more information, including limitations on which addresses and packet types can be snooped, see the *IPv6 Multicasting* chapter of the *Software Reference*.

IGMP Snooping All-Group Entry

Because IGMP is an IP-based protocol, multicast group membership for VLAN aware devices is on a per-VLAN basis. If at least one port in the VLAN is a member of a multicast group, multicast packets will be flooded onto all ports in the VLAN by default.

IGMP snooping enables the switch to forward multicast traffic intelligently on the switch. The switch listens to IGMP membership reports, queries and leaves messages to identify the switch ports that are members of multicast groups.

Multicast traffic will only be forwarded to ports identified as members of the specific multicast group.

This enhancement allows network managers to prevent specified ports from acting as IGMP all-group ports, and specify which ports are allowed to behave as all-group entry ports, by using the ENABLE IP IGMP ALLGROUP command.

For example, consider a video streaming service which has 15 channels. When the switch receives IGMP membership reports destined for the address 239.0.0.2 from an unauthorised user, all 15 channels of multicast data floods to that port, which may affect the service of the network. In order to avoid this, the network manager decides whether or not to allow a particular port to behave as an IGMP all-group port, e.g. port 8. Then, whenever the above IGMP membership report is sent, the switch will not automatically add port 8 as one of the egress ports for any IGMP membership report group, so video streaming will not get forwarded to disabled all-group ports selected by the network manager.

Commands

This enhancement modifies one command:

- SHOW IP IGMP

and has two new commands:

- ENABLE IP IGMP ALLGROUP
- DISABLE IP IGMP ALLGROUP

Modified Command

SHOW IP IGMP

Syntax `SHOW IP IGMP [COUNTER] [INTERFACE=`*`interface`*`]`

Description This command displays information about IGMP, and multicast group membership for each IP interface.

This enhancement includes the line "**Disabled All-groups ports**" on the output of this command, as show in Figure 2 on page 19. Ports that are disabled have a "#" symbol next to the port number.

Figure 2: Example output from the SHOW IP IGMP command.

```
IGMP Protocol
--------------------------------------------------------------------------------
Status ........................... Enabled
Default Query Interval ........... 125 secs
Default Timeout Interval ......... 270 secs
Disabled All-groups ports ........ 1,5,7

Interface Name .......... vlan2 (DR)
IGMP Proxy .............. Off
Group List ..............

  Group. 238.0.1.2          Last Adv. 172.50.2.1         Refresh time 34 secs
  Ports 3,11,23

  Group. 224.1.1.2          Last Adv. 172.50.2.1         Refresh time 130 secs
  Ports 2,11,23

  All Groups                Last Adv. 172.50.1.1         Refresh time 45 secs
  Ports 1#,11,23


Interface Name .......... vlan4             (DR)
IGMP Proxy .............. Off
Group List ..............
  No group memberships.

--------------------------------------------------------------------------------
```

Table 5: New parameter in the output of the SHOW IP IGMP command.

Parameter	Meaning
Disabled All-groups ports	A list of ports that are prevented from behaving as IGMP all-group ports.

Examples To show information about IGMP, use the command:

```
SHOW IP IGMP
```

See Also ENABLE IP IGMP ALLGROUP
DISABLE IP IGMP ALLGROUP

New Commands

This enhancement request introduces two new commands from enabling/ disabling all-group entries on switch ports.

ENABLE IP IGMP ALLGROUP

Syntax `ENABLE IP IGMP ALLGROUP=[{`*`port-list`*`|ALL}]`

where:

- *port-list* is a port number, a range of port numbers (specified as n-m), or a comma separated list of port numbers and/or ranges. Port numbers start at 1 ad end at m, where m is the highest numbered Ethernet switch port, including uplink ports.

Description This command enables the specified port(s) to behave as a multicast all-group ports.

The ALLGROUP parameter specifies the list of ports able to behave as all-group entry ports. If ALL is specified, all ports are able to behave as all-group entry ports. The default is ALL.

Examples To enable ports 1, 5 and 7 to behave as all-group entry ports, use the command:

```
ENABLE IP IGMP ALLGROUP=1,5,7
```

See Also DISABLE IP IGMP ALLGROUP
SHOW IP IGMP

DISABLE IP IGMP ALLGROUP

Syntax `DISABLE IP IGMP ALLGROUP=[{`*`port-list`*`|ALL}]`

where:

- *port-list* is a port number, a range of port numbers (specified as n-m), or a comma separated list of port numbers and/or ranges. Port numbers start at 1 and end at m, where m is the highest numbered Ethernet switch port, including uplink ports.

Description This command disables the specified port(s) from acting as a multicast all-group entry ports. Ports that are disabled have a "#" symbol next to the port number in the output of the SHOW IP IGMP command.

Examples To prevent ports 1, 5 and 7 from behaving as all-group entry ports, use the command:

```
DISABLE IP IGMP ALLGROUP=1,5,7
```

See Also ENABLE IP IGMP ALLGROUP
SHOW IP IGMP

Availability

Patches can be downloaded from the Software Updates area of the Allied Telesyn web site at *www.alliedtelesyn.co.nz/support/updates/patches.html*. A licence or password is not required to use a patch.